

REMARKS/ARGUMENTS

In the Office Action mailed May 29, 2009, claims 1-14 were rejected. In response, Applicants hereby request reconsideration of the application in view of the below-provided remarks. No claims are amended, added, or canceled.

Claim Rejections under 35 U.S.C. 112, first paragraph

Claims 12 and 13 were rejected under 35 U.S.C. 112, first paragraph, as purportedly failing to comply with the written description requirement. Specifically, the Office Action states that the limitation “wherein the one of the different instruction sequences is located at the program address” of claims 12 and 13 lacks support within the original disclosure.

Applicants respectfully submit that the limitation related to one of the different instruction sequences located at the program address is supported by the specification, even though there may not be explicit antecedent basis for the language. This language is supported by the specification, for example, at least on page 3, lines 3-14, which states “the desired action can be selected from a large number of possible instruction sequences by the use of a Random Number Generator” (emphasis added) and “By means of a random program run of this kind.” While the above section of page 3, lines 3-14 does not explicitly refer to the different instruction sequences located at the program address, the description at page 1, lines 14-29 describes how different instructions are associated with memory locations or program addresses. Therefore, Applicants respectfully submit that the detailed description of the specification provides support for each of these claim limitations because embodiments of the process realize jumps or branches based on conditions to determine how the instructions at each location or program address proceed.

While the specification may not explicitly provide antecedent basis for the exact language used in the claims, Applicants respectfully submit that the indicated language finds considerable support in the specification, including the support described above. See, MPEP 608.01(o) (“an applicant is not limited to the nomenclature used in the application as filed”). Furthermore, 37 C.F.R. 1.75(d)(1) requires the terms and phrases used in the claims must find clear support or antecedent basis in the description so that the meaning of the terms in the claims may be ascertainable. In other words, support is

required, and antecedent basis is simply one way of providing support, but is not the only way to provide support for the limitations of the claim.

Here, although the language of the claims differs somewhat from the actual nomenclature provided in the specification, Applicants respectfully submit that the claim language is nevertheless supported by the specification because the claims recite limitations that are well within the scope of the embodiments described in the specification. Moreover, although the MPEP indicates that the use of a variety of terms can be confusing, Applicants respectfully submit that the terms used in the claims do not cause such confusion. On the contrary, the language of the claims is ascertainable from the specification, as shown by the explanation provided above.

Therefore, Applicants assert the claims are supported by the specification as filed because the language is within the scope of the written description provided in the specification, and the language does not cause confusion as to the meaning of the claims. Accordingly, Applicants respectfully request that the rejections of claims 12 and 13 under 35 U.S.C. 112, first paragraph, be withdrawn.

Claim Rejections under 35 U.S.C. 103

Claims 1-14 were rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen (EP 0690370 A2, hereinafter Cohen) in view of Anderson et al. (U.S. Pat. Pub. No. 2003/0084336, hereinafter Anderson). However, Applicants respectfully submit that these claims are patentable over Cohen and Anderson for the reasons provided below.

Independent Claim 1

The rejection of claim 1 is improper because 1) the Office Action does not establish a *prima facie* rejection for claim 1, and 2) the proposed combination of Cohen and Anderson is improper because the proposed combination would render Cohen unsatisfactory for its intended purpose.

Lack of *Prima Facie* Rejection

In order to establish a *prima facie* rejection of a claim under 35 U.S.C. 103, the Office Action must present a clear articulation of the reason why the claimed invention

would have been obvious. MPEP 2142 (citing *KSR International Co. v. Teleflex Inc.*, 550 U.S. __ (2007)). The analysis must be made explicit. *Id.* Additionally, rejections based on obviousness cannot be sustained by mere conclusory statements; instead there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *Id.*

Here, the Office Action fails to provide an explicit reason as to why the limitations of claim 1 would have been obvious. In particular, the Office Action simply states:

Cohen does not expressly teach the use of a Random Number Generator (RNG) for purposes of microcontroller activity (e.g., controlling a Jump Condition).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Cohen as introduced by Anderson. Anderson discloses the use of a RNG for control of microcontroller activity (e.g., controlling a Jump Condition with in the microcontroller) (to provide microcontroller architecture such that the internal activities of the microcontroller are controlled by a RNG [par. 23]):

Therefore, given the teachings of Anderson, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Cohen by employing the well known feature of a microcontroller utilizing random number generation means to control its activity disclosed above by Anderson, for which microcontroller programming will be enhanced [par. 23].

Office Action, 05/29/2009, page 4.

The Office Action is merely conclusory in stating that the “microcontroller programming will be enhanced.” Applicants submit that the Office Action offers no explicit analysis to support the assertion that it would be obvious to combine the cited references, or that the indicated limitation might otherwise be obvious in light of the cited references.

Therefore, the Office Action fails to establish a *prima facie* rejection for claim 1 because the Office Action does not provide articulated reasoning with some rational underpinning in the rejection of claim 1. Accordingly, Applicants respectfully submit that the rejection of claim 1 under 35 U.S.C. 103(a) should be withdrawn because the Office Action fails to establish a *prima facie* rejection.

The Proposed Combination is Improper

Furthermore, even if the combination of Cohen and Anderson were to teach all of the limitations of the claim, the proposed combination of Cohen and Anderson is nevertheless improper. In asserting a combination of references as a basis for an obviousness rejection, the proposed combination or modification cannot change the principle of operation of the prior art. MPEP 2143.01(VI). In addition, the combination of references cannot render the prior art unsatisfactory for its intended purpose. MPEP 2143.01(V). Here, the combination of teachings proposed in the Office Action would change the principle of operation of Cohen and would render the device of Cohen unsatisfactory for its intended purpose.

The proposed combination of Cohen and Anderson is improper because the use of a random number generator, as taught by Anderson, within the device of Cohen would render the device of Cohen unsatisfactory for its intended purpose. In general, Anderson teaches protection of confidential electronic data on a microcontroller against eavesdroppers who try to reconstruct it from the electromagnetic emissions on power wires. Anderson, paragraph 1. Anderson teaches the protection of the data through “set-random-carry” commands or random “jumps” in program execution within a microcontroller to avoid data reconstruction by an eavesdropper. Anderson determines the carries, or jumps, using a pseudo-random number generator. More specifically, Anderson generates pseudo-random bits with a free-running pseudo-random number generator based on a shift register. The bit stream generated by the pseudo-random number generator is sampled upon execution of a set-random-carry command. Anderson, paragraph 23. Thus, Anderson executes a program carry, or jump, dependent on a random number bit stream sample.

Cohen also teaches causing random “jumps” in program execution to provide protection against power analysis. However, in contrast with Anderson, Cohen teaches that the performance of a conditional robust jump is dependent upon the contents and integrity of the composite condition signal within a single machine cycle. Cohen, page 8, line 43 to page 9, line 4; Fig. 7. In other words, the conditional jump is performed based on conditions within the microcontroller. More specifically, Cohen teaches that the

conditions within the microcontroller include the integrity of the data which allows a “do_jump” signal to be activated and a program jump to be executed. Thus, Cohen uses data integrity, rather than a pseudo-random number, as the criteria for the jump operation.

Nevertheless, despite the teaching of Cohen that the jump is dependent on the data integrity, the Office Action proposes to modify the teaching of Cohen to use a random number generator bit stream to trigger the jump, instead of a data integrity check. This proposition to use a random number generator not only removes the use of the code taught by Cohen (Cohen, page 9, lines 10-25) to perform a jump based on data integrity, but further would appear to eliminate the ability for the teachings of Cohen to generate the “do_jump” signal because this modification would, in turn, prevent the system from informing the outside world of a data integrity problem, as taught by Cohen.

Moreover, even if it were possible to implement the teaching of Anderson without replacing the aforementioned teachings of Cohen, the proposed modification of Cohen would also make it difficult or impossible to prevent conflicting signals from occurring with respect to controlling and tracking the jump signals because the jump criteria for Cohen and Anderson are dissimilar. Furthermore, there is no explanation of how the random number generator approach of Anderson might be implemented into the teachings of Cohen without rendering Cohen unsatisfactory for, first, communicating an error signal upon detection of a data integrity compromise and preventing a jump or branch in the microcontroller and, second, associating the jump with a signal received from an instruction decoder because Anderson teaches use of a random number generator to control jumps and branches in the program of the microcontroller.

Therefore, combining the references of Cohen and Anderson, as proposed in the Office Action, would render the device of Cohen unsatisfactory for its intended purpose because use of the bit sampling of the bit stream generated by the random number generator described in Anderson would prevent the system of Cohen from performing a jump based on data integrity and, further, would appear to prevent Cohen from generating the GoError signal which would further prevent the device of Cohen from informing the outside world of a data integrity problem. Accordingly, Applicants respectfully assert independent claim 1 is patentable over the cited references because the proposed combination of references is improper.

Independent Claims 5 and 11

Applicants respectfully assert independent claims 5 and 11 are patentable over the proposed combinations of Cohen and Anderson at least for similar reasons to those stated above in regard to the rejection of independent claim 1. Each of claims 5 and 11 recites subject matter which is similar to the subject matter of claim 1 discussed above. Although the language of these claims differs from the language of claim 1, and the scope of these claims should be interpreted independently of other claims, Applicants respectfully assert that the remarks provided above in regard to the rejection of claim 1 also apply to the rejection of these claims.

Dependent Claims

Claims 2-4, 6-10, and 12-14 depend from and incorporate all of the limitations of the corresponding independent claims 1, 5, and 11. Applicants respectfully assert claims 2-4, 6-10, and 12-14 are allowable based on allowable base claims. Additionally, each of claims 2-4, 6-10, and 12-14 may be allowable for further reasons.

CONCLUSION

Applicants respectfully requests reconsideration of the claims in view of the remarks made herein. A notice of allowance is earnestly solicited.

At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account **50-4019** pursuant to 37 C.F.R. 1.25. Additionally, please charge any fees to Deposit Account **50-4019** under 37 C.F.R. 1.16, 1.17, 1.19, 1.20 and 1.21.

Respectfully submitted,

/mark a. wilson/

Date: August 31, 2009

Mark A. Wilson
Reg. No. 43,994

Wilson & Ham
PMB: 348
2530 Berryessa Road
San Jose, CA 95132
Phone: (925) 249-1300
Fax: (925) 249-0111